

情報理論とその応用学会ニューズレター

第9回情報理論とその応用シンポジウム ワークショップ報告

Linear Dependent Process Model と情報圧縮への応用

カオス・情報・AR モデル

相原 憲一 (NTT 通研)
大石 進一 (早稲田大学)
笠原 正雄 (大阪大学)

第9回情報理論とその応用シンポジウム中
に開催された下記のワークショップ

(1) Linear Dependent Process Model と
情報圧縮への応用

(2) カオス・情報・AR モデル
について、相原氏、大石氏がそれぞれ報告書
を作成し、筆者(笠原)がそれらを要約し、
まとめる役をおおせつかった。

まず上記の順番にしたがってワークショッ
プの内容を紹介することにしよう。

「Linear Dependent Process Model
と情報圧縮への応用」(報告者:相原)

話題提供者は小林欣吾氏(大阪大学)であ
り、出席者は甘利先生(東京大学)、有本先
生(大阪大学)、井原先生(高知大学)等を
始めとする大学関係者20名、企業関係者5名
という賑やかな顔ぶれである。

物理的に直接観測できる情報系列はある関
数を通して写像されたマルコフ過程としてと
らえることができ、これを linear dependent
process(LDP)という。LDP は一般化マルコフ過
程を含んで定義され得るが、現実の世界で、

これをデータモデルとして取り扱うことが妥
当か否かが本ワークショップの主要な問題点
である。

LDP では次の行列

P: 既に観測した情報系列を表示する行列

Q: 次に観測する情報系列を予測する行列

$$Q = P^{-1} B$$

で定義される特性行列Bが重要な役割を果たす
が、この特性行列を積極的に利用してデータ
圧縮を効率的に実施することが最終目的と言
えよう。本ワークショップは小林氏の独演?
の感があったが、これに対し実際の離散的音
声、画像データ系列を LDP モデルとしてとらえ
ることが妥当か否か等についての意見が出さ
れ活況を呈した。

「カオス・情報・AR モデル」(報告者:大石)

話題提供者は大石進一氏・相澤洋二氏(早
稲田大学)であり、出席者は甘利先生(東京
大学)、古賀先生(九州大学)を始めとする
約20名の顔ぶれである。

カオスは確定系に現れる極めて複雑な振舞
いをする非線形モードであるが、このような
カオスの概念が確立されたのは1975年頃とみ
てよく、そろそろ思いもよらない素晴らしい
応用が発見されてもよい時期に到達している。

本ワークショップでは相澤氏が森敦氏編集
の「数学近未来」なる本の中でカオス応用の
新しい夢を語っていることが契機となって、
まず相澤氏が登場し、カオスの定義、夢等が
紹介された。この様な話を聞くと、赤池の情
報量基準に対する物理モデルの可能性、AR モ
デルの深層のモデル、生物の情報処理様式と
カオスの関係等々が”妄想”されるが、ワーク
ショップはこれらの話題に加えて、甘利先生
の鋭い質問、古賀先生のコメント等が述べら
れて会場は大いに盛り上がった。

以上のような内容が相原氏および大石氏より筆者に寄せられたわけである。ワークショップまとめ役としての小生は、じっくり耳を傾けて話を聞くことがもともと苦手な上、他会場で開かれているワークショップにも興味を覚えて、ホテル内を歩き回っているうちに、日本語が理解できず時間を持余しておられたLin先生につかまってしまったのである。そしてロビーで二人だけの日米情報理論ミニシンポジウムが開かれたりして、小生が担当した両会場は殆ど雰囲気がつかめぬままに終了してしまった。このようなことで報告書は文字どおりの拙文になってしまったことをおわびしたい。

公開鍵暗号ワークショップ

伊東 利哉（東京工業大学）

話題提供者 松本 勉（横浜国立大学）
黒沢 肇（東京工業大学）

公開鍵暗号ワークショップは、会場に参加者が入りきれないほどの大盛況で、40名前後の参加者により熱心な討論が繰り広げられた。

まず、横浜国大の松本先生により、ID情報に基づく方式（大規模ネットワークにおいて、ネットワーク内のセンタから各エンティティがエンティティ専用の秘密情報を受け取り、その後はセンタにアクセスすることなく、相手のエンティティのIDと自分の秘密情報を用いて暗号通信を実現する方式）として、

- (1) A. Shamir [Identity-Based Cryptosystem, Identity-Based Signature Scheme]
- (2) H. Tanaka [Modified Identity-Based Cryptosystem]
- (3) T. Matsumoto & H. Imai [Key Predistribution System]
- (4) E. Okamoto [Identity-Based Key Distribution Systems]

を中心とした話題が提供され、古典的方式、公開鍵方式に対する特徴、それぞれの利点欠点等が詳しく討論された。また、松本先生により、公開鍵方式においても、公開ファイル

を用いる代わりに、公開鍵とIDペアに対するセンタの署名を各エンティティが管理することによって、IDに基づく暗号方式を構成できることが示された。

次に、東工大の黒沢先生から、“公開鍵暗号と計算量と擬似乱数”に関する話題が提供され、暗号解読の困難さが保障された公開鍵暗号、真の乱数と多項式時間で区別することの不可能な擬似乱数の生成法に関する解説が行われた。特に、黒沢先生が最近御提案の“逆数を利用した公開鍵暗号”に対し、

(1) 暗号文から平文の最下位ビットを求める問題は、暗号文から平文全体を求めることと同程度に難しい（従って、素因数分解と同程度に難しい）

(2) 逆数暗号を用いた部分列から過去またはその未来が予測不可能な擬似乱数（従って、多項式時間で真の乱数と区別することは不可能）の生成法

等の最新の研究成果が示された。参加者の方々からは、“Yaoの定理”、“乱数の周期”等に関する活発な質問及び討論がなされた。

会場の都合によりワークショップは11時30分で打ち切られたが、議論は白熱し、まだまだ尽きる所を知らないといった雰囲気であった。御熱心な参加者の方々は、その後各部屋に戻られて、深夜に及ぶ討論をされた様子であった。

話題を提供された先生方は、大変分り易く解説して下さり、また、多くの方々が熱心に議論に参加され、今後の暗号理論、情報セキュリティに関する研究の方向を示唆する、大変貴重なワークショップであった。

光通信ワークショップ

植松 友彦（東京工業大学）

光通信ワークショップは約20人の参加を得て、電気通信大学・佐藤先生の乾杯の音頭で始まった。乾杯の後、慶応大学・中川先生、相模工業大学・広田先生による光通信の動向、量子制御理論に関する解説が行われた。中でも光通信の最大の問題となるショット雑音を

制御するために量子制御理論が生まれ、Squeezed State, Photon Number State などの量子状態が考案されたという話は圧巻であった。更に、McEliece, Massey らの符号理論の研究者が、光通信方式を提案していることが紹介され、多くの情報理論の研究者に、光通信理論への興味が喚起された。和やかな感じで、夜遅くまでワークショップは続き、光通信理論は物理・科学を推進させる力を有していることを認識すると共に、光通信理論と情報理論との間の親近感が得られ、大変有意義であった。

2次元 Berlekamp-Massey
アルゴリズムについて

山口 和彦（横浜国立大学）
今井 秀樹（横浜国立大学）

話題提供者 阪田省二郎（豊橋技術科学大学）

同日の符号理論のセッションの阪田氏の発表「与えられた2次元配列を生成する記憶素子最小の2次元線形帰還シフトレジスタの合成」に興味を持つものが待ち受ける中、阪田氏が登場して始まった。

まず、氏が話題提供者として登壇し、昼のセッションの講演の内容の詳しい説明が行われた。これに対し、終始参加者からの質問があり、氏がこれに答える形で、ワークショップはなごやかな雰囲気の中に進行した。

又関連した話題として、杉山氏（摂南大）から、阪田氏の説明に加える形で1次元のBerlekamp-Massey アルゴリズムやその解釈、関連アルゴリズムとの関係、研究の歴史などの説明があった。

話題になった点を以下にあげる。

(1) 2次元と1次元の違い。

直感的には1次元の配列を直線と見なすと、2次元は矩形を想像するが、2次元 Berlekamp-Massey アルゴリズムでは”3角形状”に与えられる2次元配列を考える。この発想から2次元のアルゴリズムが実現された。

(2) 符号理論等との対応。

2次元シフトレジスタの局部構造は、2次元巡回符号のそれと同じである。しかし1次元のBerlekamp-Massey アルゴリズムが、BCH 符号の復号法に対応するというような関係は2次元の場合にはまだ発見されていない。

一例として、代数幾何学的符号（現在効率のよい復号法が発見されていない）は、交代式符号の多次元への拡張という点で問題が似ていることがあげられた。しかし、これら相互の関連は明らかにできなかった。

(3) 他の研究分野との関連。

1次元のBerlekamp-Massey アルゴリズムとLevinson-Trennch アルゴリズムの関係のように、他の研究分野での2次元のアルゴリズムと2次元Berlekamp-Massey アルゴリズムの関係について。あるいは、他の分野でのこのアルゴリズムに関する多次元の問題の研究の有無について。

阪田氏の研究成果は上に示したように、符号理論、関連分野に新たな問題提起を与えることが確認された。しかし、今後これがどのような研究に展開してゆくのかは、この話合いでは明らかにできなかった。とくに2次元Berlekamp-Massey アルゴリズムで、復号可能な符号を求めることが、符号理論として最も重要であると考えられる。

意見がで尽くしたあと、ワークショップのテーマを離れて各参加者が現在自分の研究についての紹介を行い、情報が交換された。その一部を紹介する。常盤氏（大阪大）からはRS符号の二元重み分布の研究を現在内外での研究の進行状況、将来の動向を交えて紹介があった。このテーマに関しては、近い将来、続々研究成果が報告されるとのことである。川端氏（電通大）からは計算幾何学に関する話題の紹介があり、とくに多次元の問題の扱いについて、本ワークショップのテーマとの関連も含めた質疑が行われた。

本ワークショップの参加者は川端氏を除いて、符号理論の研究者であった。(3)の問題の解決のためにも、他の分野の研究者の参加、講演を加えた形が望まれた。この未解決の問題については、NEWSLETTER 読者にも御一考願えれば幸いである。

確立過程と信号処理ワークショップ

河野 隆二（東洋大学）
今井 秀樹（横浜国立大学）

話題提供者 長岡 浩司（東京工科大学）

定刻の9時前から19名の参加者が集まり、テーブルを輪にし、リラックスした雰囲気の中で参加者の自己紹介に続き、話題提供者の長岡氏の講演という形で始められた。講演のテーマは「多項式行列の安定性判別法とその確率過程・信号処理との関係」についてであり、長岡氏の研究成果の報告を中心に、その関連分野としての確率過程や信号処理を結びつけるものであった。

進行は、昼間のセッションとは異なり、講演中にその内容や著名な数学者に対する個人的敬慕などのランダムアクセスにより、自然な形で意見交換がなされた。講演の内容及び流れを以下に要約する。

スカラー多項式の安定性判別には、従来より連続時間については、Routh-Hurwitzの方法、離散時間については、Schur-Cohnの方法が効率よく判定できることが知られている。しかし、これをそのまま多項式行列の安定性判別に拡張することはできない。その困難さが研究の motivation である。特別な場合として、多項式行列が strictly-regular ならば、確率過程を AR process で近似 (AR fitting) するときに用いる LWR アルゴリズムは、ある意味で Schur-Cohn の方法の拡張になっている。この考え方を発展させることにより、「一般の多項式行列の安定性に関する統一的な有用な見地を得ること」が基本的思想（目的）である。

こうした研究により得られた成果をまとめると

(1) strictly-regular な離散時間多項式に関する LWR アルゴリズムが一般の column reduced 多項式行列に拡張できること。

(2) 一定の列次数を持つ column reduced な離散時間多項式行列の自由度は、安定性を決定する量とそれとは独立なある変換群に分離で

きること。

(3) reciprocal な離散時間多項式行列の安定性判別には、Schur-Cohn の方法がそのまま適用でき、安定な多項式行列は(2)の変換群の自由度を用いることにより reciprocal なものに変換できること。

(4) 連続時間多項式の安定性についても、同様の議論が可能であり、多くの場合、結果については離散時間の結果よりも簡単であること。

以上の成果、特に(3)とそれに対応する連続時間の結果より、Routh-Hurwitz の方法や Schur-Cohn の方法を多項式行列の安定性判別に拡張する上での困難さの構造及び由来が明らかになる。更に、(2)の変換群の自由度が信号処理において果たす役割については、今後の研究課題である。

結局、予定された時間内に上述の問題提起から、結果の導出までをすべて述べることはできなかった。しかし、導出の過程を大部分を除いて、明快な説明と参加者の適時の質問や意見が適度にかみ合ったと思われる。

しかし、参加者の中には、より現実的な確率過程と信号処理における話題を期待されていた方々も少なくなかった。従って、長岡氏の講演内容が上述の信号処理との関連にまで言及できるだけの十分な時間がもうけられれば更に活発な議論を行うことができたと考えられる。

以上の長岡氏の講演内容を含む研究成果は数ヶ月後に阪大に博士論文として提出される予定であり、この優れた研究成果が広範囲な分野に貢献されることを期待したい。

■ワークショップ報告はここまで■

事務局担当が大阪大学から早稲田大学に変わりました。連絡先は、ニュースレターの最終ページをご覧ください。

符号理論とその応用ワークショップ
暗号と情報セキュリティワークショップ

合同開催の御案内

標記ワークショップを下記の要領で合同開催致しますので奮って御参加下さい。

なお、WCIS'87では一部論文を公募しております。奮ってご投稿下さい。

日時： 昭和 62 年 7 月 29 日 (水) ～
7 月 31 日 (金)
7 月 29 日 (水) 10:00～12:00 WCIS'87
13:00～17:00 WCIS'87
19:00～21:00 WCIS'87
7 月 30 日 (木) 9:00～12:00 WCIS'87
13:00～18:00 WCTA'87
18:00～20:00 懇親会 (合同)
7 月 31 日 (金) 9:00～12:00 WCTA'87
13:00～18:00 WCTA'87

会場： 「東京理科大学特別教室」
(セミナーハウス)
〒278 千葉県野田市字北亀山 2669
TEL 0471-24-1501 内線 2081

交通： 東武野田線運河駅下車 徒歩 15 分
参加費： 一般 8,000 円, 学生 5,000 円
(資料代を含む。但し、一方のみに参加されても同額です)

参加申し込み:
6 月 26 日までに、下記までお申し込み下さい。尚、セミナーハウスへ宿泊をご希望の方は、同時にお申し込み下さい
(一泊 1,300 円)。

連絡先:
河野 隆二
東洋大学工学部電気工学科
電話 0492-31-1211 内線 320,332
FAX 0492-33-1855
坂庭 好一
東京工業大学工学部電気電子工学科
電話 03-726-1111 内線 2184
FAX 03-729-0685

符号理論とその応用ワークショップ
WCTA ' 87

予定内容等

ワークショップのテーマ:

- ・ 畳込み符号とその復号法
- ・ Combined Coding and Modulation

ワークショップの形式:

招待講演のみ

講演予定内容:

- (1) 畳込み符号とその復号法(概論)
- (2) Trellis coding and coded modulation
- (3) 木符号, トレリス符号, 畳込み符号
- (4) 畳込み符号とその E(R) 関数
- (5) 耐多重波変調方式
- (6) Coded modulation と Viterbi アルゴリズム
- (7) Viterbi アルゴリズムとその応用
- (8) Viterbi 復号法とその符号間干渉のある通信路への応用
- (9) 海外における Combined coding and modulation
- (10) Viterbi 復号器の装置化, LSI 化 (理論的側面) など

主催:

情報理論とその応用学会
電子情報通信学会 情報理論研究会
(誤り制御方式とその応用分科会)

協賛:

電子情報通信学会 情報セキュリティ
時限研究専門委員会

暗号と情報セキュリティワークショップ
WCIS'87

予定内容等

ワークショップの形式:

パネル討論+招待講演+公募論文

講演予定内容:

- (1) パネル討論
ID-Based システムの諸方式について

(2)招待論文のテーマ

- ①計算量理論の最近の話題 ” P=NP? ”
- ②ガロア体上の演算アルゴリズム
- ③Zero Knowledge Proof
- ④情報システムのセキュリティ評価技法

(3)公募論文のテーマ (申し込みは坂庭まで)

暗号技術の応用

＊ I C カード (Smart Card)

＊電子郵便

＊コンピュータセキュリティ
(データベースセキュリティ,
OSセキュリティを含む)

＊装置化・L S I 化

など

主催:

暗号と情報セキュリティ研究会
(C I S 研究会)

電子情報通信学会情報セキュリティ
時限研究専門委員会

協賛:

電子情報通信学会情報理論研究会
(情報セキュリティ分科会)
情報理論とその応用学会

学会シンボルマークの公募

現在、本学会の象徴にふさわしいシンボルマークを会員の皆様から募集しております。奮って御応募下さるようお願い致します。尚採用分には、SITA' 86 テレホンカードを進呈致します。

応募作品送付先・問い合わせ先:

辻井 重男

東京都目黒区大岡山 2-12-1 (〒152)
東京工業大学工学部電気電子工学科
TeL.03-726-1111 (Ext.2503)
Fax.03-729-0685

ニューズレター原稿募集

フロッピー・ディスクによる投稿を大いに歓迎いたします。この場合は、編集の都合上、一太郎による文書ファイルか MS-DOS の標準テキスト・ファイル(5'2HD,5'2DD または 8'2DD)でお願いいたします。フロッピー・ディスクは、お返し致します。

なお、投稿並びにニューズレターに関するお問い合わせは下記宛にお願いいたします。

田崎 三郎 (編集理事)

松山市文京町 3 番 (〒790)

愛媛大学工学部電子工学科

0899-24-7111 (内) 3743

韓 太舜 (編集理事)

川崎市多摩区東三田 2-2-1 (〒211)

専修大学情報管理学科

044-911-7131(内) 265

編集後記

創刊号を発行してから、あっという間に 9 ヶ月が過ぎてしまいました。現在のところ、韓-川端グループと田崎-山田グループとで 1 号おきに担当していますが、今後は編集体制を整え、有益な"情報"を積極的に発掘していく所存です。会員の皆様のご支援をお願いいたします。また、編集部としてもオリジナル企画を立案中です。ご期待下さい。

(編集幹事・山田)

情報理論とその応用学会事務局

早稲田大学理工学部堀内研究室内

東京都新宿区大久保 3-4-1 (〒160)

電話 03-209-3211(内線 3420)

FAX 03-200-2567